



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/753,842	01/08/2004	Paul Anthony Ashley	AUS920030621US1	6048

32329 7590 02/22/2007
IBM CORPORATION
INTELLECTUAL PROPERTY LAW
11400 BURNET ROAD
AUSTIN, TX 78758

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/753,842

Applicant(s)

ASHLEY ET AL.

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a). Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 01/08/04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

Art Unit: 2132

DETAILED ACTION

1. **Claims 1-18** have been examined.

Priority

2. This application does not claim priority of an application. Therefore, the effective filing data for the subject matter defined in the pending claims of this application is **01/08/2004**.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Claims 11-14 and 15-18** is rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.

5. **Claims 11-14** are directed to a computer program on a computer readable medium. The examiner asserts that the limitation of the claim raises a question as to whether or not the program is stored on an "appropriate medium" and perform the function recited on the body of the respective claims when the program is read and executed by the computer. Applicant's specification on **page 21, lines 18-22** recites that medium could include **transmission-type media, such as digital and analog communications links**. Such medium/media does not fall within the statutory classes listed in 35 USC 101. For this reason, the language of the claims raises a question as to

Art Unit: 2132

whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP § 2106 IV. B. 1(a).

6. **Claims 15-18** are directed to an apparatus for establishing a secure context for communicating message between two systems. **Furthermore, applicant's specification on page 17, lines 26-27 recites that the apparatus can be implemented as software only or can be software only.** Such apparatus does not fall within the statutory classes listed in 35 USC 101. For this reason, the language of the claims raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP § 2106 IV. B. 1(a).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2132

8. **Claims 1-18** are rejected under 35 U.S.C. 102(e) as being anticipated by **Von Arx et al** (hereinafter referred as **Arx**)(U.S. Patent No. 7,155,290 B2) (filed on Jun 23, 2003)

9. **As per independent claims 1, 6, 11, 13, 15 and 17 Arx** discloses a method for establishing a secure context for communicating messages between a first system and a second system, the method comprising:[column 8, lines 59-63] (*a communications session between external device 2/integrator/ second system and the implantable device/first device know each other's public authentication key*)

- obtaining by the second system [instigator] a first public key certificate of the first system [*Public key certificate of 1st device*], wherein the second system is able to validate the first public key certificate that contains a public key [column 12, lines 20-24, see also figure 3-4];

- Generating by the second system [instigator] a transport key, wherein the transport key is a symmetric secret key; [column 12, lines 34-40](*secret session key*) placing by the second system [instigator] the transport key [column 12, lines 34-40](*secret session key*) and an authentication token [column 12, lines 25-28, "*see "random number R_B"*") into a first message (*see column 12, lines 25-28, "third message"*) secured with the public key (column 12, lines 34-44) (*Public key of the recipient/first device*);

- Sending the first message [third message] from the second system to the first system; (*see column 12, lines 25-28, message is send from the instigator to the recipient*)

- Receiving at the second system from the first system a second message secured with the transport key in response to sending the first message to the first system; [*Figure 3-4, see "SK"*] extracting by the second system a session

Art Unit: 2132

key from the second message, wherein the session key is a symmetric secret key; and employing the session key to secure subsequent messages sent by the second system to the first system. (COLUMN 8, lines 59-63) (The session continues until one of the devices sends an end of session signal or a time-out occurs)

10. As per independent claims 2 and 7 Arx discloses a method as applied to claims above. Furthermore, Arx discloses, the method wherein, the authentication token comprises a second public key certificate of the second system, and wherein the first system is able to validate the second public key certificate. [See figure 3 and figure 4 and column 8, lines 25-50 and column 8, lines 59-column 9, line 29]

11. As per independent claims 3-5, 8-10, 12, 14, 16 and 18 Arx discloses a method as applied to claims above. Furthermore, Arx discloses, the method further comprises: decrypting, by the second system using a private key associated with the second public key certificate, a digital envelope in the second message containing the session key, wherein the digital envelope was created by the first system using a public key contained in the second public key certificate. [See figure 3 and figure 4 and column 8, lines 25-50 and column 8, lines 59-column 9, line 29]

12. Claims 1-18 are also rejected under 35 U.S.C. 102(e) as being anticipated by Peyravian M et al: (hereinafter referred as **Pey**) Title "decentralized group key management for secure multicast communications" Submitted with IDS (Published on August 1999) (Pages 1183-1187) (See Reference U)

Art Unit: 2132

13. As per claims 1-18 Pey discloses a method for establishing a secure context for communicating messages between a first system and a second system [See abstract], the method comprising:

obtaining by the second system a first public key certificate of the first system, wherein the second system is able to validate the first public key certificate that contains a public key; [page 1185, section 2.1, see point 1, in order to securely use public key the second system inherently gets/receives and verified it]

generating by the second system a transport key, wherein the transport key is a symmetric secret key; [page 1185, section 2.1, see first paragraph]

placing by the second system the transport key and an authentication token into a first message secured with the public key; sending the first message from the second system to the first system; [page 1185, section 2.1, see point 1]

receiving at the second system from the first system a second message secured with the transport key in response to sending the first message to the first system; extracting by the second system a session key from the second message, wherein the session key is a symmetric secret key; [See page 1186, section 2.2.2, the steps cited from 1-7)

and

Employing the session key to secure subsequent messages sent by the second system to the first system. (Page 1186, section 2.2.2, KD is a data encrypted key which is used for secure transmission/communication and meets the recitation of the limitation)

Conclusion

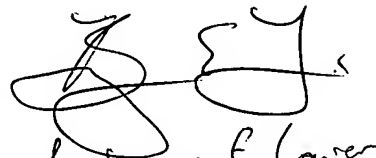
14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

Art Unit: 2132

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA*S.L.*
02/11/2007
Benjamin E. Carter
Examiner AU 2132